



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/399,192	09/17/1999	JOHN WANKMUELLER	AP31994-0704	1972

7590 08/27/2003

BAKER & BOTTS LLP
30 ROCKEFELLER PLAZA
NEW YORK, NY 101120228

EXAMINER

BACKER, FIRMIN

ART UNIT

PAPER NUMBER

3621

DATE MAILED: 08/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/399,192

Applicant(s)

WANKMUELLER ET AL.

Examiner

Firmin Backer

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 June 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Response to Amendment

This is in response to an amendment file on June 17th, 2003 for letter for patent filed on September 17th, 2003 in which claims 1-50 were presented for examination. In the amendment, claims 1, 2, 6, 10, 11-13, 17, 18, 22, 26, 27, 28, 33, 34, 38, 41-45, 49 and 50 have been amended.

Claims 1-50 remain pending in the letter.

Response to Arguments

1. Applicant's arguments with respect to claims 1-50 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-5, 17-20, 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Fak et al in view of Keil.

Re claim 1: Fak (col. 2, lines 3-11) discloses a method for generating identification data, comprising providing an ATM PIN related to a first transaction type; and performing a cryptographic operation upon an ATM PIN (i.e., derived by generating a first cipher Y1 by encrypting the account number using the PIN in combination with a first secret security number as a key). Fak et al fail to teach an inventive concept of generating a non ATM PIN for use in a

Art Unit: 3621

second transaction which is a non ATM transaction. However, Keil teaches an inventive concept of generating a non ATM PIN for use in a second transaction which is a non ATM transaction (*see abstract, paragraphs 016, 0038, 0039*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Fak et al's inventive concept to include Keil's generating a non ATM PIN for use in a second transaction which is a non ATM transaction because this would have provide a more secure system for automated transaction.

Re claim 2: Fak further discloses that the step of performing a cryptographic operation comprises: providing a conversion key (i.e., a first cipher Y1); and using the conversion key to perform said cryptographic operation upon an ATM PIN (i.e., derived by generating a first cipher Y1 by encrypting the account number using the PIN in combination with a first secret security number as a key).

Re claim 3: Fak further discloses that the step of providing a conversion key comprises: providing conversion key derivation data (i.e., PAN) providing a conversion key derivation key (i.e., PIN or a first secret security number as a key); and performing the cryptographic operation upon the conversion key derivation data and the conversion key derivation key (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claim 4: Fak further discloses that the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key (i.e., PIN or a first secret security number as a key) to perform at least one cryptographic operation upon the conversion key derivation data (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claim 5: Fak further discloses that the conversion key derivation data includes an identification number (i.e., "PAN") that is associated with multiple accounts (i.e., a bank card would inherently have multiple accounts such as saving and checking account), and wherein at least one cryptographic operation using a secret key (i.e., "a first secret security number as a key") is performed to cryptographically process said conversion key derivation data to produce the conversion key (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claims 17-20 and 33-36: The claimed system would have been inherent to perform the method disclosed by Fak as stated above.

9. Claims 6-12, 22, 23, 28, 38, 39 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Fak et al in view of Keil in further view of Konheim et al.

Re claim 6: Konheim further discloses that the step of performing a cryptographic operation comprises: providing cryptographically-computed data (i.e., "PINTRUE"); and performing an operation upon an ATM PIN (i.e., "M1") and the cryptographically-computed data (i.e., "PINTRUE").

Re claim 7: Konheim further discloses that the step of providing cryptographically-computed data comprises: providing initial data (e.g., "M1"); and performing at least one cryptographic operation (i.e., "E(K,M1)") using a secret key (i.e., "K") upon the initial data (i.e., "M1"), thereby producing the cryptographically-computed data (i.e., "PINTRUE").

Re claim 8: Konheim does not explicitly disclose that the at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

However, a DES-encryption and a DES-decryption are old and well known in the cryptographic art.

Re claim 9: Konheim further discloses that least a portion of the initial data is obtained from at least a portion of an account number (i.e., "M1 ").

Re claims 10 and 13: Konheim does not explicitly disclose that the operation upon an ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation. However, the use of a subtraction operation or an addition operation is old and well known in the cryptographic art.

Re claim 11: Konheim further discloses that the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing an ATM PIN (i.e., "PINTRUE = E(K,M1)").

Re claim 12: Konheim further discloses that the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing an ATM PIN (i.e., "PINTRUE = E(K,M1)").

Re claims 22, 23, 28, 38, 39, and 44: The claimed system would have been inherent to perform the method disclosed by Konheim as stated above.

Re claims 24-29, 40-43, and 45: The claimed system would have been obvious to perform the claimed method which would have been obvious in view of Konheim as stated above.

13. Claims 16, 32 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosenow in view of Ford et al. (Ford hereinafter: "Secure Electronic Commerce", Prentice Hall PTR, 1997).

Rosenow does not explicitly disclose the multiple encryption approach. However, Ford discloses the multiple encryption approach to enhance the security of electronic commerce (page 104). Thus, it would have been within the level of ordinary skill in the art to modify the method and system of Rosenow by adopting the teaching of Ford to enhance the security of electronic commerce.

14. Claims 21 and 37 rejected under 35 U.S.C. 103(a) as being unpatentable over Fak in view of Ford.

Fak does not explicitly disclose the multiple encryption approach. However, Ford discloses the multiple encryption approach to enhance the security of electronic commerce (page 104). Thus, it would have been within the level of ordinary skill in the art to modify the system of Fak by adopting the teaching of Ford to enhance the security of electronic commerce.

Conclusion

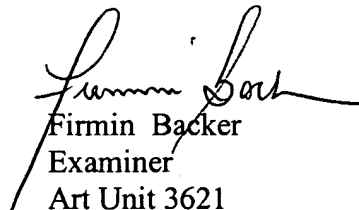
4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.


Firmin Backer
Examiner
Art Unit 3621

August 19, 2003


JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3300